

Send documentation comments to mdsfeedback-doc@cisco.com.

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 2.1(2)

Release Date: July 26, 2005

Text Part Number: OL-7411-03

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the “[Related Documentation](#)” section on [page 25](#).



Note

Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*:
http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_release_notes_list.html

Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Image Upgrade, page 5](#)
- [New Features in Cisco MDS SAN-OS Release 2.1\(2\), page 6](#)
- [Limitations and Restrictions, page 8](#)
- [Caveats, page 8](#)
- [Related Documentation, page 25](#)
- [Obtaining Documentation, page 26](#)
- [Documentation Feedback, page 27](#)
- [Cisco Product Security Overview, page 27](#)
- [Obtaining Technical Assistance, page 28](#)
- [Obtaining Additional Publications and Information, page 29](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Send documentation comments to mdsfeedback-doc@cisco.com.

Introduction

The Cisco MDS 9000 Family of multilayer directors and fabric switches offers intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. These switches combine robust and flexible hardware architecture with multiple layers of network and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9000 Family provides intelligent networking features such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 2.1(2) and includes the following topics:

- [Components Supported, page 2](#)
- [Determining the Software Version, page 5](#)

Components Supported

[Table 1](#) lists the software and hardware components supported by the Cisco MDS 9000 Family.



Note

To use the Cisco Storage Services Enabler package, Cisco MDS SAN-OS Release 1.3(5) or later must be installed on the MDS switch.

Table 1 *Cisco MDS 9000 Family Supported Software and Hardware Components*

Component	Part Number	Description	Applicable Product
Software	M95S1K9-2.1.2	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S1K9-2.1.2	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S1K9-2.1.2	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
License	M9500ENT1K9	Enterprise package.	MDS 9500 Series
	M9200ENT1K9	Enterprise package.	MDS 9200 Series
	M9100ENT1K9	Enterprise package.	MDS 9100 Series
	M9500FIC1K9	Mainframe package.	MDS 9500 Series
	M9200FIC1K9	Mainframe package.	MDS 9200 Series
	M9100FIC1K9	Mainframe package.	MDS 9100 Series
	M9500FMS1K9	Fabric Manager Server package.	MDS 9500 Series
	M9200FMS1K9	Fabric Manager Server package.	MDS 9200 Series
	M9100FMS1K9	Fabric Manager Server package.	MDS 9100 Series
	M9500EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9500 Series
	M9200EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9200 Series
	M9500EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9500 Series
	M9200EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9200 Series
	M9500EXT12K9	SAN Extension over IP package for MPS 14+2 module.	MDS 9500 Series
	M9200EXT12K9	SAN Extension over IP package for MPS 14+2 module.	MDS 9200 Series
	M9500SSE1K9	Storage Services Enabler package.	MDS 9500 Series with ASM or SSM
	M9200SSE1K9	Storage Services Enabler package.	MDS 9200 Series with ASM or SSM
Chassis	DS-C9509	MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs ¹ sold separately).	MDS 9509 only
	DS-C9506	MDS 9506 director (6-slot modular chassis includes 4 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9506 only
	DS-C9216-K9	MDS 9216 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216 only
	DS-C9216A-K9	MDS 9216A 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216A only
	DS-C9216i-K9	MDS 9216i 16-port semi-modular fabric switch (includes 14 1-Gbps/2-Gbps Fibre Channel ports, 2 Gigabit Ethernet ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216i only
	DS-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 only
	DS-C9140-K9	MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 host-optimized ports).	MDS 9140 only

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 1 *Cisco MDS 9000 Family Supported Software and Hardware Components (continued)*

Component	Part Number	Description	Applicable Product
Supervisor modules	DS-X9530-SF1-K9	MDS 9500 Supervisor/Fabric-I, module.	MDS 9500 Series only
Switching modules	DS-X9016	MDS 9000 16-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series
	DS-X9032	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	
Services modules	DS-X9308-SMIP	8-port Gigabit Ethernet IP Storage Services module.	
	DS-X9304-SMIP	4-port Gigabit Ethernet IP Storage Services module.	
	DS-X9032-SMV	32-port Fibre Channel Advanced Services Module (ASM).	
	DS-X9032-SSM	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM).	
	DS-X9560-SMC	Caching Services Module (CSM).	
	DS-X9302-14K9	14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module.	
LC-type fiber-optic SFP	DS-SFP-FC-2G-SW	2-Gbps/1-Gbps Fibre Channel — short wavelength SFP.	MDS 9000 Family
	DS-SFP-FC-2G-LW	2-Gbps/1-Gbps Fibre Channel — long wavelength SFP.	
	DS-SFP-FCGE-SW	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—short wavelength SFP.	
	DS-SFP-FCGE-LW	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel — long wavelength SFP.	
CWDM ²	CWDM-SFP-xxxx-2G	Gigabit Ethernet and 1-Gbps/2-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm.	MDS 9000 Family
	CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths.	
	CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths.	
	CWDM-CHASSIS-2	Two slot chassis for CWDM add/drop multiplexer(s).	
Power supplies	DS-CAC-300W	300-W ³ AC power supply.	MDS 9100 Series only
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only
	DS-CDC-2500W	2500-W DC power supply.	
	DS-CAC-4000W-US	4000-W AC power supply for US (cable attached).	
	DS-CAC-4000W-INT	4000-W AC power supply international (cable attached).	
	DS-CAC-1900W	1900-W AC power supply.	MDS 9506 only
	DS-CDC-1900W	1900-W DC power supply.	
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB.	MDS 9500 Series only

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Port analyzer adapter	DS-PAA-2	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric.	MDS 9000 Family
CD-ROM	M90FM-CD-212=	MDS 9000 Management Software and Documentation CD-ROM, spare	MDS 9000 Family

1. SFP = small form-factor pluggable
2. CWDM = coarse wavelength division multiplexing
3. W = Watt

Determining the Software Version



Note

We strongly recommend that you use the latest available software release supported by your vendor for all Cisco MDS 9000 Family products.

To determine the version of the Cisco MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch using the CLI, log into the switch and enter the **show version EXEC** command.

To determine the version of the Cisco MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch using the Fabric Manager, view the Switches tab in the Information pane, locate the switch using the IP address, logical name, or WWN, and check its version in the Release column.

Image Upgrade

The Cisco MDS SAN-OS software is designed for mission-critical high availability environments. To realize the benefits of nondisruptive upgrades on the Cisco MDS 9500 Directors, we highly recommend that you install dual supervisor modules.

You can nondisruptively upgrade to Cisco MDS SAN-OS Release 2.1(2) from any SAN-OS software release beginning with Release 1.3(x). If you are running an older version of the SAN-OS, upgrade to Release 1.3(x) and then Release 2.1(2).

When downgrading from Cisco MDS SAN-OS Release 2.1(2) to Release 1.3(x), you might need to disable new features in Release 2.1(2) for a nondisruptive downgrade. Issuing the **install all** command from the CLI, or using Fabric Manager to perform the downgrade enables the compatibility check. The check indicates that the downgrade is disruptive and the reason is “current running-config is not supported by new image.”

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
2	yes	disruptive	reset	Current running-config is not supported by new image
3	yes	disruptive	reset	Current running-config is not supported by new image
5	yes	disruptive	reset	Current running-config is not supported by new image
6	yes	disruptive	reset	Current running-config is not supported by new image

Send documentation comments to mdsfeedback-doc@cisco.com.

At a minimum, you need to disable the default device alias distribution feature using the **no device-alias distribute** command in global configuration mode. The **show incompatibility system bootflash:1.3(x)_filename** command determines which additional features need to be disabled.



Note

Refer to the “Determining Software Compatibility” section of the *Cisco MDS 9000 Family Configuration Guide* for more details.

New Features in Cisco MDS SAN-OS Release 2.1(2)

This section describes the new features introduced in this release. For more information about the features listed, refer to the *Cisco MDS 9000 Family Configuration Guide* and the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.



Note

This release note is specific to this release. For the Cisco MDS SAN-OS Release 2.x documentation set, see the “[Related Documentation](#)” section on [page 25](#).

Nondisruptive Storage Services Module (SSM) Image Upgrade

You can perform a nondisruptive upgrade of Fibre Channel switching for an SSM using the new **install ssi** command. The SSM must be running EPLD version 2.1(2) to use the **install ssi** command. To upgrade the EPLD image, the SSM must be installed on a Cisco MDS 9500 Series switch.

Default Initial State for SSMs

Storage Service Modules (SSMs) initially come up in Fibre Channel switching mode by default.

Persistent FC IDs and Domains for IVR

You can configure persistent FC IDs and domains for IVR. This improves IVR management by allowing you to control and assign a specific virtual domain to use for a native VSAN, and by allowing you to control and assign a specific virtual FC ID to use for a device.



Note

The ability to configure persistent FC IDs and domains for IVR is supported in Cisco MDS SAN-OS Release 2.1(2) through the CLI. Support for this feature in Fabric Manager will be available in MDS SAN-OS Release 3.0(1).

SCSI Flow Services Support for Interfaces

You can configure SCSI flow services on groups of four interfaces, as well as on the entire module.

Send documentation comments to mdsfeedback-doc@cisco.com.

Special Characters in TACACS+ Global Secret Keys

Two special characters are allowed in TACACS+ global secret keys. You can use the dollar sign (\$) and the percent sign (%) in TACACS+ global secret keys.

Control for SNMP Notifications for linkUp/linkDown Traps

In Cisco MDS SAN-OS Release 2.1(2), users can configure which linkUp/linkDown trap notifications to enable for interfaces.

NASB Storage Array Controller Support

You can enable Network-Accelerated Serverless Backup (NASB) as storage array controller devices.

NASB Target Rediscovery

You can enable Network-Accelerated Serverless Backup (NASB) to rediscover a target device.

iSCSI Duplicate WWN Check

You can check for potential WWN conflicts in the current configuration.

Fabric Manager Enhancements

The Cisco MDS 9000 Family Fabric Manager supports:

- Fabric Manager Web Services. Fabric Manager Web Services enhancements include:
 - Custom report generation.
 - License inventory.
 - TACACS+ authentication.
 - Enhanced Traffic Analyzer integration.
 - SNMP user management.
- SAN Extension Tuner wizard.
- Export topology map to Vision.
- Automatic host enclosure creation.
- Java run-time environment (JRE) 1.5.0 support.
- Performance Manager. The Performance Manager allows performance reports to be rolled up by host-optimized port groups and host or storage enclosures.
- Cisco MDS 9000 FabricWare. Cisco Fabric Manager supports switches running Cisco FabricWare.

Send documentation comments to mdsfeedback-doc@cisco.com.

Limitations and Restrictions

The maximum number of targets that SANTap supports is 16.

For the latest VSFN compatibility information, refer to the *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*.

Caveats

This section lists the open and resolved caveats for this release. Use [Table 2](#) to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

Table 2 *Open Caveats and Resolved Caveats Reference*

DDTS Number	Software Release (Open or Resolved)	
	2.1(1a)	2.1(2)
Severity 2		
CSCef11644	O	R
CSCed57251	O	R
CSCeg11095	O	R
CSCeg12962	O	R
CSCeg20932	O	R
CSCeg90336	O	O
CSCeh29872	O	R
CSCeh39705	O	R
CSCeh41378	O	R
CSCeh49483	O	R
CSCeh52973	O	O
CSCeh61610	O	R
CSCeh64080	O	R
CSCeh70727	O	R
CSCeh71865	O	R
CSCeh73149	O	O
CSCeh85768	O	R
CSCeh87930	O	R
CSCeh90270	O	R
CSCeh91293	O	R
CSCeh92604	O	O
CSCeh93109	O	O
CSCeh93625	O	R
CSCeh95139	O	R

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 2 *Open Caveats and Resolved Caveats Reference (continued)*

DDTS Number	Software Release (Open or Resolved)	
	2.1(1a)	2.1(2)
CSCeh96928	O	R
CSCei01431	O	R
CSCei02196	O	R
CSCei03442	O	R
CSCei10774	O	O
CSCei17870	O	R
CSCei18830	O	O
CSCei18837	O	R
CSCei19822	O	O
CSCei25319	O	R
CSCei40874	O	O
CSCei49569		R
CSCei50818	O	O
CSCei52477	O	R
CSCei53783	O	O
CSCei55208	O	R
CSCei55341	O	O
CSCin93539	O	O
CSCin95832	O	O
Severity 3		
CSCec31365	O	O
CSCed14920	O	R
CSCed16845	O	O
CSCef56229	O	O
CSCef87845	O	R
CSCeg01551	O	R
CSCeg12383	O	O
CSCeg27584	O	O
CSCeg37598	O	O
CSCeg55238	O	O
CSCeg53114	O	R
CSCeg66225	O	R
CSCeg72539	O	R
CSCeg84853	O	R
CSCeh08307	O	R

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 2 *Open Caveats and Resolved Caveats Reference (continued)*

DDTS Number	Software Release (Open or Resolved)	
	2.1(1a)	2.1(2)
CSCeh19639	O	R
CSCeh31983	O	R
CSCeh33814	O	R
CSCeh33448	O	R
CSCeh33548	O	O
CSCeh34275	O	R
CSCeh34828	O	O
CSCeh35859	O	R
CSCeh36025	O	R
CSCeh37066	O	R
CSCeh38055	O	R
CSCeh38123	O	R
CSCeh40138	O	R
CSCeh41947	O	R
CSCeh52280	O	R
CSCeh56143	O	R
CSCeh65824	O	R
CSCeh71894	O	R
CSCeh73101	O	R
CSCeh75500	O	O
CSCeh79330	O	R
CSCeh82166	O	R
CSCeh82490	O	R
CSCeh83514	O	R
CSCeh87985	O	R
CSCeh88814	O	O
CSCeh92843	O	R
CSCei08541	O	R
CSCei17687	O	R
CSCei18425	O	R
CSCei22596	O	R
CSCei29086	O	R
CSCei31020	O	R
CSCei32317	O	O
CSCei48889	O	O

Send documentation comments to mdsfeedback-doc@cisco.com.

Table 2 *Open Caveats and Resolved Caveats Reference (continued)*

DDTS Number	Software Release (Open or Resolved)	
	2.1(1a)	2.1(2)
CSCei50995	O	R
CSCei57761		R
CSCin87497	O	R
CSCin92030	O	R
CSCin92870	O	O
CSCin95686	O	O
CSCin95789	O	O

Resolved Caveats

- CSCef11644

Symptom: VPN 4.0.1 does not work with large SNMP PDU packets.

Workaround: Upgrade to VPN 4.0.5.

- CSCed57251

Symptom: In some rare instances in Cisco MDS SAN-OS Release 1.3, 2.0, and 2.1(1), when the IP Storage Services (IPS) module restarted after a failure, VSAN membership information about iSCSI interfaces was lost. However, a configuration saved with the **copy running-config startup** command was not lost.

Workaround: None.

- CSCeg11095

Symptom: Duplicate fabrics are opened under different SANs when the loadFromDB option is selected.

Workaround: In Fabric Manager, select **Admin > Fabrics** to remove the fabric, and then reopen it with the loadFromDB box deselected.

- CSCeg12962

Symptom: Some hosts may not accept IKE tunnel creation from Cisco MDS 9000 Family switches when an IKE session already exists in the switch. In such cases it may take more than the expected time for the IPsec session to come up. This scenario can happen when the Gigabit Ethernet interface on the switch fails and comes back up or if you issue a VRRP switchover to a different switch.

Workaround: For a faster recovery, disconnect and reinitiate the iSCSI session from the host.

- CSCeg20932

Symptom: If an IPS module with operational FCIP PortChannels is reloaded, upgraded, or downgraded, the supervisor module may be reloaded causing the system to reboot.

Workaround: Before reloading, upgrading, or downgrading an IPS module, shut down all FCIP PortChannels on the line card.

- CSCeh29872

Symptom: The ICMP Path-MTU discovery might not work with IPsec depending upon the SPD policy that is created and where the ICMP error message is originated.

Send documentation comments to mdsfeedback-doc@cisco.com.

Workaround: Identify the path MTU and set it as the local interface MTU in the switch.

- CSCeh39705

Symptom: iSCSI immediate and unsolicited data is not allowed to be used when the data digest is turned on.

Workaround: None.

- CSCeh41378

Symptom: If an MDS switch has more than one module that supports Ethernet ports, the Cisco Discovery Protocol (CDP) learns entries over both the Gigabit Ethernet ports and the mgmt0 port. Subsequently, if there is either a system switchover or a restart of the CDP process, CDP will lose neighbors learned over the Gigabit Ethernet ports. A side effect of this behavior is that the **sh cdp neighbors interface <gig intf>** command causes the CDP process to crash and results in either a switchover on a dual supervisor or a reload on a single supervisor. This problem does not occur as long as the MDS switch is populated with just one module that supports Ethernet ports. Any combination of two or more modules supporting Ethernet ports will cause the problem. In addition, in the case of the Cisco MDS 9216i a module that supports Ethernet ports along with the supervisor module in slot1 is susceptible to the problem.

Workaround: None. Disable CDP so it does not learn of any entries, thereby preventing a crash or switchover.

- CSCeh49483

Symptom: Traffic stops flowing when a member, who is not the first member, of a non-trunking PortChannel in an IVR zone set is flapped.

Workaround: None.

- CSCeh52973

Symptom: The switch appears in two VSANs when connected through ISL.

Workaround: None.

- CSCeh61610

Symptom: FCIP write acceleration does not work with HDS TagmaStore(UPS) Truecopy.

Workaround: None.

- CSCeh64080

Symptom: Following an upgrade from Release 1.1 to Release 1.3 or higher, with persistent FC ID enabled, the FC IDs for the storage arrays may get changed after a link flap.

Workaround: None.

- CSCeh70727

Symptom: When many iSCSI sessions go up or down simultaneously, such as when a line card fails, the amount of syslog messages generated can overwhelm the supervisor and cause a new iSCSI session login to be delayed.

Workaround: None.

- CSCeh71865

Symptom: If two IPS ports on an IPS module are configured in the same IP subnet, but put on different LAN segments, external iSNS clients may not be able to connect to the iSNS server on the IPS port.

Workaround: Put the IPS ports in the same IP subnet on the same LAN segment.

- CSCeh85768

Send documentation comments to mdsfeedback-doc@cisco.com.

Symptom: During an upgrade of the firmware on an IBM tape drive, the tape utility program may hang after it resets and performs loop initialization. The tape drive sends OPN, FLOGI, and CLS. The switch sends OPN and ACC, but does not send CLS, which causes the tape utility to hang while it waits for CLS.

Workaround: After the firmware is correctly upgraded on the tape drive, follow these steps:

- Disable the switch port using the **shut** command.
- Enable the switch port using the **no shut** command.

- CSCeh87930

Symptom: A newly configured FCIP link may fail to come up when running on an MPS-14/2 module. This symptom may occur following an upgrade of Cisco MDS SAN-OS Release 2.0(1b) to Release 2.0(3) and the configuration of a new FCIP link.

In the log on the switch, you may see the following messages:

```
%PORT-5-IF_DOWN_ELP_FAILURE_ISOLATION: %$VSAN xyz%$ Interface fcipabc is down
(Isolation due to ELP failure)
%PORT-5-IF_DOWN_OFFLINE: %$VSAN xyz%$ Interface fcipabc is down (Offline)
%PORT-5-IF_DOWN_NONE: %$VSAN xyz%$ Interface fcipabc is down (None)
```

VSAN xyz is the allowed VSAN number for the FCIP interface and interface fcipabc is the configured FCIP interface number.

Workaround: Reload the MPS-14/2 module using the **reload module *module-number*** command, where *module-number* is a specific module.

- CSCeh90270

Symptom: Two MDS 9000 switches configured with an FCIP bridge port (B port) tunnel may have problems with multi-frame sequences. You may notice this problem activating large zone sets when the SFC frame times out.

Workaround: If the connection is between two MDS switches, then the B port configuration is not required and should not be used. If B port is a requirement, then reduce the zone set length by not distributing the full database, or use VSANs.

- CSCeh91293

Symptom: The output from the **fcping** and **tracert** commands shows an incorrect MDS 9000 switch and password for enclosure fabrics.

Workaround: None.

- CSCeh93625

Symptom: The line cards shut down after the supervisor module fails.

Workaround: Remove the failed supervisor module and reinsert the line card. Or enter the **no poweroff module *slot*** command in Exec mode on the switch, where *slot* is the slot number of the module that failed.

- CSCeh95139

Symptom: If a Fibre Channel target goes offline while an iSCSI login is occurring, the IPS port will terminate the TCP session, but it will not return a login response PDU to the iSCSI initiator. As a result, some iSCSI initiators wait up to 30 seconds before they try to log in again.

Workaround: None.

- CSCeh96928

Send documentation comments to mdsfeedback-doc@cisco.com.

Symptom: If you have configured your switch port for auto speed using the **switchport speed auto** command and auto mode using the **switchport auto mode** command, the switch port may fail to establish a link with the device connected through an Emulex HBA LP8000 and remains in a link-failure state. The problem occurs with the following combination of HBA, driver, firmware, and OS configured at 1 Gbps.

Workaround: Configure the switch port speed to 1 Gbps using the **switchport speed 1000** command to support the Emulex HBA LP8000.

- CSCei01431

Symptom: An FCIP interface stays in the initializing state if it is part of a PortChannel and it is removed with the **no fcip enable** command.

Workaround: Remove the PortChannel that the FCIP interface previously belonged to.

- CSCei02196

Symptom: When a default zoning policy is permitted and there is no active zone set, packets may drop on Fx ports if there are a lot of Fx and Nx ports going up and down.

Workaround: Configure and activate a zone set.

- CSCei03442

Symptom: A core dump is generated when a chassis reloads and multiple modules do not reboot in a reasonable amount of time. The system health monitor on a module is restarted by the process manager resulting in the core dump.

Workaround: None.

- CSCei10774

Symptom: Disabling QoS does not remove the QoS attribute from an IVR zone set, and subsequent activation of the IVR zone set will not succeed.

Workaround: Remove the QoS attribute from the IVR zone set, both active and configured, before disabling QoS.

- CSCei17870

Symptom: WWNs assigned to iSCSI initiators by the system can inadvertently be returned to the system when an upgrade fails or a manual downgrade is performed, such as when an older iSAN software version is booted up without using the **install all** command. In these scenarios, the system can later assign those WWNs again to other initiators, which causes conflicts. This bug is a duplicate of [CSCeg53114](#).

Workaround: When a scenario like this occurs, Cisco MDS SAN-OS Release 2.1(2) prevents the problem by reserving any configured WWNs that belong to the system. In addition, users can check for potential conflicts in the current configuration using the **iscsi duplicate-wwn-check** command.

- CSCei18837

Symptom: If the standby supervisor and the line cards are reloaded simultaneously, the line cards do not come online and reach the OK state.

Workaround: Perform a reload at the switch level to recover from this problem.

- CSCei25319

Symptom: An error message in the log file occurs because the platform manager component passes the wrong parameter while responding to an SNMP query. In some cases, this results in the query not being responded to.

Workaround: Perform a refresh on the Device Manager to clear the problem.

Send documentation comments to mdsfeedback-doc@cisco.com.

- CSCef87845

Symptom: The CFS merge status as shown by the **show cfs merge status name app-name** command output may not reflect the correct merge status on certain switches while two fabrics are merging.

CFS merge is a protocol that runs between a designated switch in either fabric. Other switches do not participate in the merge process. While a merge is happening, the switches not merging do not reflect this, only the designated switches have the correct information. Once the merge is done, all switches would show the correct status. Usually, the merge completes in a very short time and this behavior is unlikely to be noticed.

Workaround: None.

- CSCeg01551

Symptom: If you issue a **dpvm commit** command, the DPVM application implicitly activates the existing configuration database. The configuration database is activated only when the **dpvm commit** command is explicitly issued after the **dpvm activate** command.

Workaround: None.

- CSCeg53114

Symptom: WWNs assigned to iSCSI initiators by the system can inadvertently be returned to the system when an upgrade fails or a manual downgrade is performed, such as when an older iSAN software version is booted up without using the **install all** command. In these scenarios, the system can later assign those WWNs again to other initiators, which causes conflicts. This bug is a duplicate of [CSCei17870](#).

Workaround: When a scenario like this occurs, Cisco MDS SAN-OS Release 2.1(2) prevents the problem by reserving any configured WWNs that belong to the system. In addition, users can check for potential conflicts in the current configuration using the **iscsi duplicate-wwn-check** command.

- CSCeg66225

Symptom: Password recovery might fail if you use the **copy <config-url> startup** command to save the switch configuration, or if you boot a system image that is older than the image you used to store the configuration and did not use the install all command. The following message might display in syslog or on the console during the process of password recovery.

```
<<%ASCII-CFG-2-ACFG_CONFIGURATION_APPLY_ERROR>>
```

Workaround: Issue the write erase command from the switchboot prompt.



Note Using the write erase command will erase the configuration. You must reapply the configuration, if externally stored, after the switch login.

- CSCeg72539

Symptom: iSNS server functionality may not restore iSCSI initiator node detail properly after a system switchover. Under this circumstance, iSNS server will not respond correctly to DevGetNext request from an iSNS client. This problem does not happen consistently.

Workaround: None

- CSCeg84853

Symptom: If two fabrics merge, one with automatic VSAN topology and the other configured VSAN topology, and if the autonomous fabric ID assignment as per the user configured topology is not the same as the autonomous fabric ID assignment in the autonomous fabric ID table then sometimes the IVR zone set activation keeps waiting for the switch with the lowest WWW to modify the AFID table to correct the misconfiguration.

Send documentation comments to mdsfeedback-doc@cisco.com.

Workaround: Issue the **clear ivr session** command to clear the IVR session and reactivate the IVR zone set followed by the **ivr commit** command.

- CSCeh08307

Symptom: The Fabric Manager server does not filter VSANs by each client's VSAN scope.

Workaround: None.

- CSCeh19639

Symptom: Alias for a down endport is not shown and is referenced by its pwwn in the Edit FullZoneset screen of the Fabric Manager rather than the fcalias name. This does not affect the functionality of adding those members to the zones either in Fabric Manager or in the CLI.

Workaround: None

- CSCeh31983

Symptom: The **boot** command accepts **modflash://slot-0/**, even though an image should not be stored on modflash://slot-0/. If it is, the image disappears upon SSM reload.

Workaround: Store an SSI image on the SSM flash on modflash://slot-1/ (where *slot* is the slot number where SSM is installed) and have the SSI boot variable point to modflash://slot-1/.

- CSCeh33814

Symptom: The RMON_ALERT e-mail does not send the variable or any information about what alarm is triggered.

Workaround: None.

- CSCeh33448

Symptom: The **show version image** command does not support the use of modflash:.

Workaround: Copy the image back to the supervisor to execute the **show version image** command.

- CSCeh34275

Symptom: iSCSI initiators do not advertise their iqn names on Interop VSAN Fibre Channel name server (FCNS). Fabric Manager will not display them.

Workaround: None.

- CSCeh35859

Symptom: After a process restart or merging with several fabrics simultaneously, the IVR zoneset activation process might hang in the "ready to advertise" state.

Workaround: Clear the IVR session by issuing the **clear ivr session** command and then reactivate the IVR zoneset by issuing the **ivr zoneset activate name < name> force** followed by the **ivr commit** command.

- CSCeh36025

Symptom: iSNS server continues giving a list of iSCSI targets that are in the VSAN of an iSCSI interface even after iSCSI VSAN membership feature is disabled.

Workaround: Explicitly put all iscsi interfaces in VSAN 1 before disabling iscsi interface vsan-membership.

- CSCeh37066

Symptom: If you have an SSM with Fibre Channel write acceleration enabled, flapping a port during heavy I/Os causes the data plane processor (DPP) software to drain all the pending I/Os. If the draining process takes too long, it can result in timeouts for reconfiguration of the affected SCSI flows.

Send documentation comments to mdsfeedback-doc@cisco.com.

- Workaround:** After port flapping is finished, disable the SCSI flow features and reenable them.
- CSCeh38055

Symptom: In the running-configuration output, the **zoneset activate name zoneset_name vsan vsan** command appears after the **ivr zoneset activate name zoneset_name** command. Hence, if a saved running-configuration is applied, then IVR zone set activation without the force option would fail if there is no active regular zone set when the **ivr zoneset activate** command is issued from the running configuration.

Workaround: Issue the **ivr zoneset activate name <name> force** command one more time followed by **ivr commit**.
- CSCeh38123

Symptom: If IVR NAT mode is enabled, avoid IVR zone members within transit VSANs. In rare cases, IVR devices might not be able to communicate with each other when the IVR zone set has members in transit VSANs and when there are multiple parallel transit VSANs.

Workaround: None.
- CSCeh40138

Symptom: If an IVR-enabled fabric (fabric A) running Cisco MDS SAN-OS Release 2.0 merges with an IVR-enabled fabric (fabric B) running Cisco MDS SAN-OS Release 2.0 or higher, then the IVR process on fabric A may restart if fabric B contains only an active IVR zone set but no configured zone sets.

Workaround: Make sure that fabric B has at least one IVR zone set configured if it has just one active IVR zone set.
- CSCeh41947

Symptom: Following SSA1 losing sync, the switch resets SSA0 rather than SSA1, prior to sending a sync loss message to the supervisor. The crossbar manager reports a sync loss and a successful resync on either fabric 0 link1 or fabric 1 link1, but traffic does not flow to or from the line card.

Workaround: Reload the line card. Because this problem only occurs when sync loss has occurred, the loss of sync could indicate a hardware problem with the line card, the chassis, or the fabric.
- CSCeh52280

Symptom: A corrupted license file installs on an MDS 9000 switch without errors.

Workaround: None.
- CSCeh56143

Symptom: A Fabric Manager zone migration wizard causes a Telnet session to hang when a non-MDS switch is present.

Workaround: None.
- CSCeh65824

Symptom: If you install an SSM and boot it with either the VSFN or SSI image, the Enterprise License grace period starts.

Workaround: None.
- CSCeh71894

Symptom: An infotrend storage loop device does not perform fabric login (FLOGI) after failover testing.

Workaround: Reinitialize the link in this state and provide stimulus to the loop device to log in again.

Send documentation comments to mdsfeedback-doc@cisco.com.

- CSCeh73101
Symptom: When you perform a nondisruptive upgrade from Release 1.3(x) to 2.0(x), and then issue the **show running-config** command, the switch displays the wrong user. The user shown will be inconsistent with the user shown when you issue the **show user-account** command.
Workaround: Recreate the user.
- CSCeh79330
Symptom: Exception logs occur on a syslog verification. These are caused by repacking the fm.jar and fmserver.jar files. The Device Manager now requires the fmserver.jar file for a syslog RMI registry inquiry.
Workaround: None.
- CSCeh82166
Symptom: MDS switches in SAN islands appear under several logical domain SANs.
Workaround: None.
- CSCeh82490
Symptom: An MDS 9000 switch running SAN-OS 2.0(1b) can potentially send excessive Call Home messages due to a malfunctioning line card that acts as if it were being inserted and removed repeatedly.
Workaround: None.
- CSCeh83514
Symptom: After upgrading to Release 2.0, it is no longer possible to create, modify, or delete the admin role.
Workaround: Before upgrading to Release 2.0, create the admin role.
- CSCeh87985
Symptom: When no role is associated with a user, SNMP fails when the **no role name admin** command is issued to delete the admin role. The SNMP user (admin) has no roles assigned, which causes the failure when there is an attempt to delete a specific role.
Workaround: Associate at least one role (group) to the user by executing the **snmp-server user username [group-name]** command in config mode.
- CSCeh92843
Symptom: When an iSCSI host sends a read command to a target and some Fibre Channel data-in frames are not received by an IPS line card but the MDS switch receives a good SCSI status frame from the target, the IPS port can send an iSCSI status PDU with a wrong Status Sequence Number (StatSN) to the iSCSI host, causing it to reset the TCP connection. This scenario has been observed in some rare instances of Fibre Channel cable cut testing.
Workaround: None.
- CSCei08541
Symptom: If there are two FCIP members in the PortChannel, while the traffic is running (at a 1-Gbps rate or any other large rate) bring up the second FCIP link (previously just one FCIP member is up), and you will see the total PortChannel throughput drop to about 10% of the previous number, and this low rate will last for about 25 seconds.
Workaround: None.
- CSCei17687

Send documentation comments to mdsfeedback-doc@cisco.com.

Symptom: FLOGI service may fail after a switchover due to high availability inconsistency caused when a VSAN, enabled with FICON, is deleted and recreated. The VSAN configuration events should occur before the switchover. The process of bringing up the F port after the switchover triggers the FLOGI service termination. This scenario is very rare and is caused by some race conditions within the FLOGI service.

Workaround: None.

- CSCei18425

Symptom: Fabric Manager does not display FCIP tunnels properly.

Workaround: None.

- CSCei22596

Symptom: When a special frame is enabled for FCIP and FCIP is bound to an Ethernet channel, the IPS port may fail. The failure results if FCIP TCP connections need to be migrated to the peer core and then TCP on the new peer core must be initialized properly.

Workaround: Disable the special frame in FCIP.

- CSCei29086

Symptom: Following the installation of a third-party syslog server to a PC running Fabric Manager and Device Manager, the third-party syslog server takes ownership of the PC's IP address as the syslog server. As a result, the MDS switch is no longer able to act as the syslog server.

You can see the error message "java.lang.NullPointerException" if you verify syslog on the MDS switch through Device Manager by choosing **Logs > Syslog > Verify**.

If you uninstall the third-party software and verify syslog again with **Logs > Syslog > Verify**, you see the error message "Can't connect to FM server."

Workaround: To allow the MDS 9000 switch to be the syslog server, follow these steps:

1. Stop or uninstall the third-party syslog server.
2. Stop Fabric Manager and Fabric Manager Web Services through Windows by right-clicking **My Computer > Manage > Services and Applications > Services**.
3. Restart Fabric Manager.

- CSCei31020

Symptom: If more than one path is configured for an explicit path, the running configuration shows one path, even when there are other paths. If the explicit path is not used for any FC-tunnel interface, then there is no problem.

Workaround: Copy the running configuration to a network file or onto bootflash. Manually add the paths that are present in the running configuration to the files.

- CSCei50995

Symptom: Ports are shown incorrectly in the MIB. In the CISCO-FCIP-MGMT-MIB, connUnitNumPorts should show only FC ports in the system. In the CISCO-FC-FE-MIB, fcFeModuleFxCapacity should show only the number of FC ports. For the MPS-14/2 module, Ethernet ports are also shown incorrectly. This caveat supersedes CSCeh74379.

Workaround: None.

- CSCei55208

Symptom: In some rare cases, an IVR process may restart if VSANs with IVR devices are continuously suspended and unsuspended while IVR zone set activation is in progress.

Send documentation comments to mdsfeedback-doc@cisco.com.

Workaround: Avoid suspending and unsuspending VSANs with IVR members while IVR zone set activation is in progress.

- CSCei57761

Symptom: An HP blade server is recognized as a storage device by Fabric Manager.

Workaround: Manually set the HP blade server to a host device.

- CSCin87497

Symptom: Cisco MDS SAN-OS Release 2.1(1a) does not support in-order delivery (IOD) for QoS attribute changes in IVR traffic. However, QoS for IVR traffic is supported, along with IOD for IVR traffic in all other cases.

Workaround: None.

- CSCin92030

Symptom: The Performance Manager web client displays incorrect average and peak values. In such cases, values are higher than what is shown in the web client display.

Workaround: None.

- CSCin92870

Symptom: The Fabric Manager server does not automatically handle a fabric merge and split. As a result, you may see duplicate fabrics in the database and the web client.

Workaround: Close all fabrics from the Fabric Manager Server and then reopen the new fabric.

Open Caveats

- CSCeg90336

Symptom: A user that you create in Fabric Manager or Device Manager cannot log in from the console. Release 2.1(2) fixes this problem. However, if a third-party application creates a user using SNMP, a new MIB is required for Release 3.0.

Workaround: Third-party applications should use SSH to connect to the MDS 9000 switch, and then use CLI commands to create the user account.

- CSCeh73149

Symptom: The VSAN suspend/resume operation facilitates network level reconfiguration and is not often used. In MDS SAN-OS Release 2.1(2), the command should not be used on SANTap related VSAN.

Workaround: If VSAN suspend/resume must be used, first unprovision SANTap prior to using VSAN suspend/resume.

- CSCeh92604

Symptom: Enabling IVR-NAT on the same switch where write acceleration is enabled over a PortChannel of multiple FCIP links might result in frames from the source to the destination not transferring.

Workaround: Do not have all of the following on the same switch:

- IVR-NAT enabled
- PortChannel of multiple FCIP links that can potentially carry IVR-NAT traffic
- FCIP write acceleration

However, any two of the above three configurations are supported on the same switch.

Send documentation comments to mdsfeedback-doc@cisco.com.



Note IVR in non-NAT mode can be configured with FCIP PortChannels and FCIP write acceleration on the same switch.

- CSCeh93109

Symptom: When SANTap is unprovisioned without the appliance first deleting objects it had previously created, SANTap may have problems if the session objects are present.

Workaround: The appliance must delete all objects first before SANTap is unprovisioned.

- CSCei18830

Symptom: Removing zones from an active zone set may generate a system message that the zone activation has failed due to an Accept Change Authorization (ACA) failure.

Workaround: None required. The IVR retries the activation and eventually the zone set activation succeeds.

- CSCei19822

Symptom: An active IVR zone set on the local switch is not propagated when the commit session contains any other configuration changes.

Workaround: For Release 2.1(2), perform an implicit commit without any changes. In the case of a merge failure and the IVR zone set is not active on remote switches but is active on a local switch, issue an implicit commit from the local switch to propagate the active zone set to the remote switches.

For releases prior to 2.1(2), the workaround is different. Add either a dummy member to an existing zone or add a dummy zone with dummy members to the currently active IVR zone set, and then reactivate the IVR zone set. Then issue the **commit** command, which will propagate the active zone set to other switches.

- CSCec31365

Symptom: When IVR is enabled, the Fabric-Device Management Interface information is not transferred across VSANs for IVR devices.

Workaround: None.

- CSCed14920

Symptom: During a switch upgrade, a SAN Volume Controller (SVC) node may not save its entire state under rare circumstances. This results in that node not being part of the cluster after the switch upgrade. Verify this symptom by issuing the **show nodes local** command at the `svc-config` prompt—the command output displays the following information:

- The `cluster state` of the affected SVC node is `unconfigured`.
- The `node state` of the affected SVC node is `free`.

Workaround: Manually remove the SVC node from the cluster and then add the node back into the cluster. Refer to the *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide* for procedural details.

- CSCed16845

Symptom: Occasionally, the Common Information Model (CIM) server may be automatically restarted due to an internal error. In this case, the connected CIM client is disconnected.

Workaround: You must explicitly reconnect the CIM client to the CIM server.

- CSCef56229

Send documentation comments to mdsfeedback-doc@cisco.com.

Symptom: If an iSCSI initiator is configured differently on multiple switches, iSNS might report more targets to the initiator than the initiator can access. An iSCSI initiator would get a target error if it attempts to establish a connection.

Workaround: None.

- CSCeg12383

Symptom: On rare occasions, the PortChannels with FCIP interface members fail to come up when the switch reboots. This happens when the startup configuration has a default switchport trunk mode setting that does not match the configured trunk mode for PortChannel members (FCIP interfaces). Also, the startup configuration shows any explicit switchport trunk mode setting for the PortChannel.

Workaround: Reconfigure the switchport trunk mode on the PortChannel.

- CSCeg27584

Symptom: Creating a role that has VSAN policy as “deny” requires an Enterprise License on the switch. If such a role is created on a switch that does not have the license, the switch exhibits different behavior when distribution is turned on versus when distribution is turned off.

- If distribution is turned off, creation of the role is rejected.
- If distribution is turned on, creation of the role succeeds but the VSAN policy continues to be “permit.”

Workaround: None.

- CSCeg37598

Symptom: The iSNS server might crash when iSCSI is disabled and iSNS is enabled using Fabric Manager.

Workaround: None.

- CSCeg55238

Symptom: Files created using the **fcanalyzer local** command cannot be copied or viewed. FC analyzer runs as root and the files that it creates are created with the owner as root. The correct file creation masks are not set when the file is created and so no user other than root can read or copy the file.

Workaround: None

- CSCeh33548

Symptom: Tape devices can only be accessed over an FCIP tunnel in a PortChannel with write acceleration enabled if SID/DID based load-balancing is used in the VSANs.

Workaround: Disable write acceleration or enable SID/DID based load-balancing in the VSANs if you have tape device traffic going over a FCIP tunnel in a PortChannel.

- CSCeh34828

Symptom: If there are active IVR zones with the QoS attribute, then QoS should not be disabled (for example, with the **no qos enable** command or through Fabric Manager).

Workaround: Before disabling QoS, QoS attributes from the active IVR zones should be removed and then the resultant IVR zone set should be reactivated.

- CSCeh75500

Symptom: A device that interfaces with SANTap may request SANTap to create a session for an ITL that was previously requested, and ITL checking is not robust.

Send documentation comments to mdsfeedback-doc@cisco.com.

- Workaround:** Have the device validate the ITL and ensure that it does not send a request for a duplicate ITL.
- CSCeh88814

Symptom: When SANTap is unprovisioned, the control virtual target (CVT) object is not getting cleaned up on the supervisor module.

Workaround: To ensure that cleanup occurs, the administrator should first issue the **no santap module slot-number appli-vsantap vsan-id** command to clean up the CVT, and then unprovision SANTap.
- CSCei32317

Symptom: When configuring a remote SPAN (RSPAN), the Fibre Channel tunnel will not come up if it goes through more than one hop.

Workaround: Configure the Fibre Channel tunnel explicit-path option and list every IP hop between the source and destination.
- CSCei40874

Symptom: If port 9001 is in use by another process, the database update for the previous release tables and data may hang.

Workaround: Edit the server.properties file in the bin directory and use another port. Alternatively, remove the process that opened port 9001.
- CSCei48889

Symptom: LTO tape drives in the IBM-3584 library are not supported. When multiple initiators (such as Backup Host and NASB engine) issue SCSI write commands to this tape drive, it responds with a SCSI CHECK CONDITION with Sense = 0x03 and ASC/ASCQ = 0x3b/0x00. It does not handle the transition from the host initiator to the NASB engine initiator. In general, this is an issue for all NASB solutions with this tape drive and library combination. This behavior pertains only to the LTO drives on the IBM 3584 library. LTO-2 drives on the same library function correctly.

Workaround: None.
- CSCei49569

Symptom: An IVR zoneset activation fails at any IVR enabled switch and remains in "ready to advertise" state. This happens in very rare cases when the force option is not used while activating the IVR zoneset.

Workaround: Deactivate IVR zoneset from an IVR enabled switch where the IVR Zoneset activation status is either "ready to advertise" or "advertising". Note that this step would disrupt IVR traffic. When the deactivation is successful then reactivate the IVR zoneset with the force option.
- CSCei50818

Symptom: iSCSI hosts are unable to log in to the target storage arrays because of name server issues on the IPS blade.

Workaround: None.
- CSCei52477

Symptom: During a single CLI session, if a user repeatedly (over 6000+ times) enters a nested submode and exits all submodes using the **end** command, the system will crash.

Workaround: Log out of the session and log in again before continuing operations.
- CSCei53783

Symptom: An iSCSI host cannot log in to one IPS port after many supervisor module switchovers.

Send documentation comments to mdsfeedback-doc@cisco.com.

Workaround: None.

- CSCei55341

Symptom: Undefined objects are found in CISCO-VLAN-MEMBERSHIP-MIB.

Workaround: None.

- CSCin93539

Symptom: Following the merge of two fabrics, the Fabric Manager Client cannot open.

Workaround: Close all fabrics and reopen the new fabric.

- CSCin95686

Symptom: The RRD graph in the Performance Manager does not refresh on a web client opened in Mozilla or Netscape.

Workaround: Do not use a proxy server or use the browser's Refresh button.

- CSCin95789

Symptom: When you configure Cisco Traffic Analyzer to capture traffic on one or more interfaces on a Windows platform, the configuration web page might not show that the interface has been selected for traffic capture even though traffic capture on that interface is enabled.

Workaround: Check the logs to clarify that the correct interface has been selected.

- CSCin95832

Symptom: An installation of the Device Manager following the installation of the Fabric Manager failed the install process was trying to detect the port that will be used by the database server. If the port is taken, the installation displays an error and then quits. By default, the database tries to bind to port 9001. If the port is taken by another application, the database cannot be started.

Workaround: Do not check the database server port during installation. If the port is not available and the database server cannot be started, the database updating dialog box hangs. If that occurs, follow these steps to resolve the problem.

1. Terminate the database updating process.
2. Modify the server.properties file in theInstallation_directory/bin/ to specify another available port.
3. Repeat the installation.

Send documentation comments to mdsfeedback-doc@cisco.com.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents:

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Interoperability Support Matrix*
- *Cisco MDS SAN-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*
- *Cisco MDS SAN-OS Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family SSM Configuration Note*
- *Cisco MDS 9000 Family ASM Configuration Note*
- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*
- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9020 Fabric Switch Hardware Installation Guide*
- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Family Fabric and Device Manager Online Help*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*
- *Cisco MDS 9000 Family Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9020 Fabric Switch MIB Quick Reference*
- *Cisco MDS 9000 Family CIM Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9020 Fabric Switch System Messages Reference*
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

For information on VERITAS Storage Foundation™ for Networks for the Cisco MDS 9000 Family, refer to the VERITAS website: <http://support.veritas.com/>

Send documentation comments to mdsfeedback-doc@cisco.com.

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website:
<http://www.ibm.com/storage/support/2062-2300/>

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Send documentation comments to mdsfeedback-doc@cisco.com.

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com
- Nonemergencies — psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Send documentation comments to mdsfeedback-doc@cisco.com.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

Send documentation comments to mdsfeedback-doc@cisco.com.

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

Send documentation comments to mdsfeedback-doc@cisco.com.

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

[tap://www.cisco.com/go/acclimatizing](http://www.cisco.com/go/acclimatizing)

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and entrants. You can access the Internet Protocol Journal at this URL:

[tap://www.cisco.com/apt](http://www.cisco.com/apt)

- World-class networking training is available from Cisco. You can view current offerings at this URL:

[tap://www.cisco.com/en/US/learning/index.html](http://www.cisco.com/en/US/learning/index.html)

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2004 - 2005 Cisco Systems, Inc. All rights reserved.